Google Inc. et al v. Egger et al
Doc. 472 Att. 3

EXHIBIT Q

Dockets.Justia.com

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON

AL-HARAMAIN ISLAMIC FOUNDATION, INC., et al. Plaintiffs, v. GEORGE W. BUSH, et al. Defendants.	Case No: 3:06-cv-00274-KI

SUPPLEMENTAL DECLARATION OF FRANCES R. HOURIHAN

I, Frances R. Hourihan, declare as follows:

(1) I am a special agent with the Federal Bureau of Investigation ("FBI") assigned to the FBI Washington Field Office, Washington, D.C. I have been a special agent with the FBI since July 1998. This declaration supplements my April 11, 2006 declaration previously submitted in this matter and is intended to provide additional detail about the FBI's investigation concerning the classified document that was inadvertently disclosed by a government employee without proper authorization.

(2) The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) In late August 2004, FBI headquarters received notification that a government document containing classified information had been improperly disclosed to a private party without authorization. ~~On~~ August 31, 2004, after receipt of that notification, the ~~FBI Washington Field Office~~ initiated an investigation to determine the nature and circumstances of the unauthorized disclosure to private counsel for the Al-Haramain Islamic Foundation in Oregon, in connection with that group being designated as "Specially Designated Global Terrorist" pursuant to the

International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1701-1706, and Exec. Order No. 13,224.

(4) Based on information developed in the investigation, the FBI determined that the disclosure of the classified government document occurred on or about August 20, 2004, and was unauthorized and inadvertent. During the investigation, it was determined that an employee of the Office of Foreign Assets Control ("OFAC"), a Department of Treasury component, inadvertently included the classified government document in a group of unclassified documents that the government employee had assembled and subsequently produced to private counsel in connection with the Treasury designation of the Al-Haramain Islamic Foundation.

(5) Prior to the inadvertent disclosure, this classified information had been properly maintained in a secure facility at the Department of Treasury. The FBI investigation showed that the assigned workspace of the government employee who disclosed the classified information, as well as the secure storage for the classified document, were both located within an approved Sensitive Compartmented Information Facility (SCIF) maintained by the Department of Treasury. The investigation also showed that the government employee assembled and copied the unclassified documents intended for disclosure while working within the secure SCIF space. During the unclassified document assembly process and while within the SCIF, the classified document, which was related to the terrorist designation, was inadvertently copied by the government employee and inadvertently included with the unclassified OFAC materials that were collected for disclosure to private counsel. The FBI investigation therefore determined that the original classified government document remained stored within the SCIF maintained by the Department of Treasury.

(6) In early October 2004, after approximately six weeks of a non-public national security investigation, the FBI made the determination that the unauthorized disclosure was inadvertent and not the result of a knowing or intentional unauthorized disclosure. Because the first weeks of this investigation were devoted to discovering the source and motivation, if any, for the disclosure, the FBI's investigation was necessarily non-public. This initial, non-public FBI national security investigation was necessary for several reasons including, but not limited to, the

investigative need to: determine the facts and circumstances relating to this unauthorized disclosure without alerting potential subject(s), known or unknown, to the existence or scope of the investigation which would provide the opportunity to destroy, conceal or alter evidence; identify the full scope of the unauthorized disclosure; assess whether the unauthorized disclosure was an isolated event or an indication of a broader intentional compromise; conduct a security risk assessment of the involved government employees; and make the investigative determination whether the unauthorized disclosure was or was not an intentional or knowing unauthorized disclosure of classified information to a Specially Designated Global Terrorist with the intent to harm the national security of the United States. The FBI could not make efforts to retrieve the classified document during this stage because its investigation would have been thereby publicized, undermining law enforcement and investigative efforts.

(7) At the conclusion of the non-public aspect of the national security investigation, FBI personnel with appropriate government security clearances were able to begin the process of retrieving copies of the classified government document from persons not authorized to have possession of the classified document. As noted in my previous declaration, several people who were identified as having unauthorized access to the government document were interviewed by the FBI. See Decl. of Frances R. Hourihan ¶¶ 5-7 (Apr. 11, 2006). Each person interviewed was asked to return all copies of the classified document; asked to identify the location of any copies of the document not in their possession; and advised that they should not further review, disclose, discuss, retain and/or disseminate the classified document or the classified information contained in the document. During this phase of the investigation the following individuals were among those interviewed: Lynne Bernabei was interviewed on October 07, 2004; Wendell Belew was interviewed on October 14, 2004; and Asim Ghafoor was interviewed on October 13, 2004, November 01, 2004, and November 03, 2004. Finally, the copies of the classified document retrieved by FBI personnel were transported by FBI special agents with appropriate government security clearances to a secure and limited access FBI facility that is approved for the storage of classified government materials.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Frances R. Hourihan
Special Agent
Federal Bureau of Investigation
Washington, D.C.

Executed this 10th day of May, 2006.

EXHIBIT R

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Lynne Bernabei, Esq.
The Bernabei Law Firm, PLLC
1775 T Street, NW
Washington, DC 20009-7124

VIA FACSIMILE

Thomas Nelson, Esq.
Box 1211
24525 E. Welches Rd.
Welches, OR 97067

FEB 06 2008

Re: Al Haramain Islamic Foundation, Inc.-Oregon and Soliman al-Buthe

Dear Ms. Bernabei and Mr. Nelson:

I write in response to Ms. Bernabei's letter of January 4, 2008, and in furtherance of our letter to you of November 14, 2007, which provided notice that OFAC was considering redesignating Al Haramain Islamic Foundation, Inc.-Oregon ("AHIF-Oregon") and Soliman al-Buthe. As set forth below, after a thorough investigation and review of the evidence in the record regarding AHIF-Oregon and Mr. al-Buthe, OFAC has determined that AHIF-Oregon and Mr. al-Buthe continue to meet the criteria for designation under Executive Order 13224 ("Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism") ("E.O. 13224") and, based on an updated and revised Administrative Record, including submissions by your clients, they are hereby redesignated. Accordingly, AHIF-Oregon's and Mr. al-Buthe's pending requests for delisting are denied. Separately, please see the last section of this letter for an update concerning OFAC policy on the use of blocked funds for the payment of legal expenses.

Redesignation

In reaching the decision to redesignate, OFAC has considered the following: (1) all communications between OFAC and your offices or other counsel on behalf of AHIF-Oregon and Mr. al-Buthe, including submissions made both prior to and following the original designation in September 2004; (2) a revised version of the initial designation memorandum and supporting exhibits; and (3) additional unclassified, privileged, and classified information. As you have requested, all of the submissions you have made on behalf of AHIF-Oregon and Mr. al-Buthe have been incorporated into the Administrative Record. The additional unclassified material OFAC has obtained and reviewed in response to AHIF-Oregon's petition for reconsideration (in addition to the unclassified material upon which the original designation was based) has been provided to you previously and will also be available to you in the course of the litigation associated with this matter.

Your arguments related to why AHIF-Oregon should not be designated pursuant to E.O. 13224 primarily consist of the following:

- AHIF-Oregon was an independent organization that was involved exclusively in charitable activities and was not involved in the support of terrorism, Specially Designated Global Terrorists, or other alleged supporters of terrorism;
- AHIF-Oregon funds transferred to AHIF in Saudi Arabia for use in Chechnya were not used to support terrorism, but rather in support of AHIF/Saudi Joint Relief Committee activities in Chechnya that were approved of by the Russian Government;
- AHIF-Oregon's distribution of Islamic literature was constitutionally protected activity and not an appropriate basis for designation.

After considering your arguments and submissions, and reviewing the whole Administrative Record, I have determined that the Administrative Record compiled by OFAC provides reason to believe that AHIF-Oregon meets the criteria for designation pursuant to E.O. 13224 on the following bases: (1) being owned or controlled by SDGTs Aqeel al-Aqil and al-Buthe, (2) acting for or on behalf of SDGTs al-Aqil and al-Buthe, and (3) supporting and operating as a branch office of AHIF, an international charity that employed its branch offices to provide financial, material, and other services and support to al Qaida and other SDGTs.[1] Among the information relating to AHIF-Oregon supporting the redesignation is the fact that two of the founding directors of AHIF-Oregon were -- and remain — Specially Designated Global Terrorists, namely Mr. al-Buthe, who was the Treasurer of AHIF-Oregon, and Mr. al-Aqil, who was the founding President of both AHIF-Oregon[2] and AHIF in Saudi Arabia. Both classified and unclassified reporting indicates that the AHIF parent organization in Saudi Arabia, and in particular Mr. al-Aqil himself, maintained strong and direct control over activities of the branches. Mr. al-Aqil himself confirmed in a 2002 interview that the AHIF parent organization in Saudi Arabia maintained "tight control" over its branches.

Substantial classified and limited unclassified reporting, including the Staff Report to the National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing that Ms. Bernabei provided to OFAC in 2004 for consideration, reveals the extent and nature of AHIF's longstanding and significant support, through its international branches, of SDGTs and terrorist activity around the world, including al Qaeda and the mujahideen in Chechnya, and dating back as far as the 1998 bombings of the U.S. Embassies in Kenya and Tanzania. AHIF-Oregon was an active arm of this worldwide organization, and its operations, including its direct provision of funding to AHIF in Saudi Arabia,[3] enabled the global AHIF to continue supporting terrorist activities. Finally, your arguments regarding AHIF activities in Chechnya were considered, but rejected in light of the classified and unclassified administrative record.

---

[1] AHIF-Oregon's distribution of Islamic literature is not a basis upon which AHIF-Oregon has been redesignated, nor was it a basis for the designation in September 2004.

[2] As set forth in Ms. Bernabei's correspondence of August 4, 2004, Mr. al-Aqil and another senior al Haramain official, Mansur al-Kadi, purportedly submitted formal resignations from the AHIF-Oregon board in 2003. Nevertheless, classified and unclassified information indicates that Mr. al-Aqil retained effective control over the activities of all branches until his departure from AHIF in 2004, and according to some reports, even following his purported departure from the parent organization.

Additional Issues Raised by AHIF-Oregon

I would also like to respond to several concerns raised in Ms. Bernabei's January 4, 2008 letter.[4] First, Ms. Bernabei indicates that there is no basis in E.O. 13224 or the applicable regulations for a redesignation. A redesignation is, in essence, a process whereby OFAC updates and supersedes its original designation on the basis of a revised administrative record. OFAC undertakes the redesignation process pursuant to the same standards as apply to any designation action under E.O. 13224. Specifically, OFAC analyzed the applicability of designation criteria set forth in section 1 of the E.O. based on all information currently available to it. OFAC also provided AHIF-Oregon notice of the pending determination and allowed AHIF-Oregon to provide any additional information it wished OFAC to consider. In the end, this redesignation has provided more process for the benefit of AHIF-Oregon than would have been provided were OFAC simply to have amended the original designation record administratively, which, as Ms. Bernabei points out, the OFAC regulations provide for.

In sum, we are confident that the redesignation process — particularly when considered in light of the extent of materials provided to you by OFAC during the original designation process, as well as the willingness of OFAC to accept numerous submissions from AHIF-Oregon for consideration and incorporation into the administrative record — has provided AHIF-Oregon with a constitutionally sound level of due process, as several courts have found in analogous circumstances. *See Holy Land Found. v. Ashcroft*, 219 F. Supp. 2d 57, 77 (D.D.C. 2002), *aff'd* 333 F.3d 156, 163 (D.C. Cir. 2003); *Islamic American Relief Agency v. Unidentified FBI Agents*, 394 F. Supp. 2d 34, 49 (D.D.C. 2005), *aff'd in part and remanded*, 477 F.3d 728 (D.C. Cir. 2007); *Global Relief Found., Inc. v. O'Neill*, 207 F. Supp. 2d 779, 804 (N.D. Ill. 2002), *aff'd*, 315 F.3d 748 (7th Cir. 2002). Of particular note, the Holy Land Foundation raised claims nearly identical to those in Ms. Bernabei's letter when it challenged OFAC's redesignation. The court rejected these arguments and upheld the redesignation. *See Holy Land Found.*, 219 F. Supp. 2d at 76, n.29.

Second, the January 4 letter also raises concerns about the unclassified, non-privileged materials provided to you. Specifically Ms. Bernabei asserts that not every exhibit pertains to AHIF-Oregon or AHIF in Saudi Arabia. OFAC is entitled to consider the full panoply of relevant information available to it, and all the information provided to you either relates directly to AHIF-Oregon or AHIF or provides context for such other information. *Cf. Holy Land Found.*, 333 F.3d at 162 ("it is clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations"). Moreover, OFAC is aware of the concerns presented by any media reporting, foreign and domestic, and considers the reliability of such reporting when relying upon such information.

---

[3] Both Ms. Bernabei's correspondence of September 21, 2005, and the Complaint filed challenging AHIF-Oregon's designation, admit such direct funding of AHIF in Saudi Arabia. *See. e.g.*, Compl. ¶ 63.

[4] As this matter is currently in litigation, this letter only touches upon several of the matters raised in the January 4 correspondence. OFAC reserves the right to provide responses in the litigation to any arguments raised by AHIF-Oregon in the litigation.

In many cases, the media reporting provided to AHIF-Oregon has been used in conjunction with classified materials. OFAC's use of classified information is provided for by statute and has been upheld by numerous courts. *See* 50 U.S.C. § 1702(c); *Global Relief Found. v. O'Neill*, 207 F. Supp. 2d 779, 791 (N.D. Ill.), *aff'd*, 315 F.3d 748, 754 (7th Cir. 2002); *Islamic American Relief Agency v. Gonzales*, 394 F. Supp. 2d 34, 45 (D.D.C. 2005), *aff'd* 477 F.3d 728 (D.C. Cir. 2007); *Holy Land Found. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003).

Third, OFAC and the Department of Justice requested that each agency that provided classified information used by OFAC in the redesignation process review that information to determine whether it remained appropriately classified. After several months of close coordination with multiple agencies, OFAC has been informed that, as of the date of this letter, all classified material used in the final Administrative Record remains properly classified.

In sum, as stated above, AHIF-Oregon and Mr. al-Buthe are thus redesignated, and all pending requests for delisting are hereby denied. This constitutes final agency action on this matter. A copy of the unclassified version of the evidentiary memorandum will follow shortly under separate cover.

Use of Blocked Funds for Legal Expenses

Regarding the use of blocked funds for payment of legal expenses, OFAC has recently adopted a policy to authorize the release of a limited amount of blocked funds for the payment of legal fees and costs under certain circumstances. Specifically, the policy would allow a limited amount of blocked funds to be released for the payment of legal fees and certain costs incurred in seeking administrative reconsideration or judicial review of the designation of a U.S. person pursuant to the Global Terrorism Sanctions Regulations, 31 C.F.R. Part 594. Accordingly, the policy would potentially apply to your representation of AHIF-Oregon.

In order to complete the processing of your license request(s) pursuant to this policy, OFAC requests the following information:

- The hourly rate and number of hours billed per attorney for legal services directly related to the request for administrative reconsideration of the designation and the legal challenge thereto, divided by each phase of the case (i.e., administrative filings to OFAC and proceedings at the district court);

- An itemized statement and description of costs incurred in seeking administrative reconsideration or judicial review of AHIF-Oregon's designation;
- A certification, signed under penalty of perjury, that AHIF-Oregon has no assets, property, or economic resources of any type outside the United States, and does not have access to any AHIF funds worldwide; and
- A certification that to the best of your knowledge the blocked funds do not represent the property interest of another or serve as security for other obligations of AHIF-Oregon.

OFAC will evaluate your request(s) for the release of blocked funds for payment of attorney fees and costs incurred in seeking administrative reconsideration and judicial review of AHIF-Oregon's designation pursuant to the policy upon receipt of the information requested.

Sincerely,

Adam J. Szubin
Director
Office of Foreign Assets Control

PUBLIC-AR 2201

086

EXHIBIT S

Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

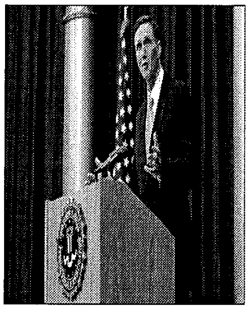
Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Major Executive Speeches



John S. Pistole
Deputy Director
Federal Bureau of Investigation

American Bankers Association/American Ba
Association Money Laundering Enforcement
Conference
Washington, D.C.

October 22, 2007

Note: The Deputy Director may deviate from prepared remarks

Good morning. It's an honor to be here today to talk about terrorist financing and how it affe law enforcement business and the banking business.

Today I want to give you an overview of terrorist financing and walk you through the FBI's pr conducting terrorist financing investigations. And finally, I'd like to talk about how important a are to the FBI's counterterrorism mission.

* * *

Money is the lifeblood of terrorism. Without it, terrorists cannot train, plan, communicate, bu equipment, or execute their attacks. But with it, they can do immeasurable damage. And so always looking for ways to fly below the radar, hoping to stay unnoticed and unsuspected wh turn their plans into a reality.

We learned this lesson the hard way on September 11, 2001. The 9/11 hijackers wanted to unnoticed, and their financial transactions did fly below our radars. It wasn't until after the att when we began backtracking through their finances—that red flags went up.

We discovered that the hijackers used the formal banking system freely and even shared ac accounts. We were able to track their everyday purchases at places like Wal-Mart and their throughout the country. Things that might not have registered before suddenly took on enorn significance. For example, they had no Social Security numbers. They moved their money i relatively small, non-suspicious amounts, using mainly wire transfers and credit and debit ca transactions and some cash transactions.

But they didn't engage in any complex financial tradecraft to conceal their activities. Instead, looked for weaknesses they could exploit. For instance, they sent structured wire transfers fi institutions that had no software or program in place to detect them. One financier simply us alias to wire money, because he knew the sending bank didn't have a robust "Know Your Cu program.

Our financial investigation conclusively linked the hijackers together. But it is not enough to financial autopsy after an attack. It became clear that the law enforcement and intelligence

088

Good morning. It's an honor to be here today to talk about terrorist financing and how it affects the law enforcement business and the banking business.

. Today I want to give you an overview of terrorist financing and walk you through the FBI's process of conducting terrorist financing investigations. And finally, I'd like to talk about how important all of you are to the FBI's counterterrorism mission.

* * *

Money is the lifeblood of terrorism. Without it, terrorists cannot train, plan, communicate, buy equipment, or execute their attacks. But with it, they can do immeasurable damage. And so they are always looking for ways to fly below the radar, hoping to stay unnoticed and unsuspected while they turn their plans into a reality.

We learned this lesson the hard way on September 11, 2001. The 9/11 hijackers wanted to remain unnoticed, and their financial transactions did fly below our radars. It wasn't until after the attacks—when we began backtracking through their finances—that red flags went up.

We discovered that the hijackers used the formal banking system freely and even shared access to accounts. We were able to track their everyday purchases at places like Wal-Mart and their travels throughout the country. Things that might not have registered before suddenly took on enormous significance. For example, they had no Social Security numbers. They moved their money in relatively small, non-suspicious amounts, using mainly wire transfers and credit and debit card transactions and some cash transactions.

But they didn't engage in any complex financial tradecraft to conceal their activities. Instead, they looked for weaknesses they could exploit. For instance, they sent structured wire transfers from institutions that had no software or program in place to detect them. One financier simply used an alias to wire money, because he knew the sending bank didn't have a robust "Know Your Customer" program.

Our financial investigation conclusively linked the hijackers together. But it is not enough to conduct a financial autopsy after an attack. It became clear that the law enforcement and intelligence communities needed to find early opportunities to identify and to disrupt terrorist networks. The best way to do that is to scrutinize finances.

When terrorists raise, store, move, and spend money, they leave trails. They are complex—but they are traceable and identifiable through global financial systems.

The financial analysis of the September 11 hijackers gave us a better idea of what to look for. It helped us establish new intelligence requirements and set up new tripwires. We established a specialized section in our Counterterrorism Division called the Terrorism Financing Operations Section, or TFOS.

The mission of our agents and analysts in TFOS is to trace transactions and track patterns. This painstaking work helps us identify, disrupt, and prosecute terrorists, their associates, their leaders, and their assets.

* * *

Let me give you a sense of how we conduct terrorist financing investigations and what we're looking for. But just a quick reminder that predication is the key to every investigation we undertake. We are not out looking at everyone's finances for no reason. In fact, when it comes to terrorist financing, it is often you who provide the predication for our investigations.

First and foremost, we're looking for basic personal information—addresses, birthdates, phone numbers, and employment. These help us understand day-to-day expenses and spending habits. This information then helps us uncover travel patterns, other accounts, important transactions, and financial histories. And these in turn may lead us to previously unknown business or personal associations, including other members of a network. They may also lead us to discovering criminal activity, such as IRS violations or money laundering.

In short, the most basic financial investigative techniques can result in a gold mine of intelligence.

But we don't want to do a financial autopsy after an attack has occurred. Instead we want to conduct proactive investigations—and we are.

For example, we investigate charities or non-governmental organizations that are used to generate and move money around the world. Some of them fraudulently obtain charitable donations and then divert them to support terrorism.

This was the case with the Benevolence International Foundation in Chicago. It claimed to provide relief to widows and orphans—and it did in fact use some of its funds to provide humanitarian assistance. But the organization was actually a front for al Qaeda. The Executive Director pled guilty to racketeering conspiracy and is now serving 11 years in federal prison.

We also investigate traditional criminal activity that might be used to support terrorism. Because of the crackdown on terrorists and their supporters, terrorists are not necessarily getting stipends from al Qaeda. Instead, they are raising it themselves, often through garden-variety crimes.

For example, the Madrid bombers sold drugs and pirated CDs. A group in North Carolina smuggled cigarettes and used the profits to fund Hezbollah in Lebanon. And in Torrance, California, members of a terrorist cell robbed gas stations so they could buy weapons and plan attacks against Jewish targets and U.S. military installations in Los Angeles. And so we must always be looking for links among traditional crimes and terrorist activities.

Another type of case is one in which we investigate facilitators—the people who move the money, whether witting or unwitting. In addition to using the traditional banking system, terrorists and their supporters also take advantage of unregistered Money Service Businesses and hawalas. These appeal to terrorists and their supporters for obvious reasons. One does not need to be an existing customer to use them.

Hawalas are informal remittance systems that operate primarily within ethnic communities. They can be operated from any location with a phone and Internet hookup, whether it is a gas station or a private home. They don't operate by any of the rules of the financial sector. There is no one to regulate anything. Hawalas are based on trust and offer near-anonymity for those who are trying to avoid scrutiny. In one case, we investigated a hawala that had sent approximately $4 million to over 20 different customers in foreign countries.

* * *

The 9/11 hijackers proved that terrorists and their supporters are always looking for chinks in the armor of our financial systems. We've made tremendous progress in the past six years in making it much harder for them to raise and move money. A big part of this is thanks to you.

Just like criminals and their money launderers, terrorists and their support networks rely on secrecy to conduct their business. If their activities can be monitored and flagged, they can potentially be stopped. We in the FBI can't do our jobs without the help and cooperation of the banking industry.

You are the gatekeepers of information about terrorists' financial activity. Your compliance with reporting requirements, subpoenas, and other requests for information are absolutely vital to our efforts.

The stronger our systems are, and the closer our coordination is, the better our chances at detecting and stopping terrorists before they can act.

Records produced and maintained pursuant to the Bank Secrecy Act are especially vital weapons in our arsenal—particularly Suspicious Activity Reports and Currency Transaction Reports. Every single one of our terrorism investigations has a financial sub-file—and one of the first things on our checklist is to query FinCEN for BSA reports that match the subject. You would be amazed at how much valuable intelligence they produce—especially SARs and CTRs.

As we have seen since the September 11th attacks, terrorists don't necessarily need huge sums of money to plan and carry out an attack. In a sample of FBI cases, about 42 percent of subjects had BSA reports filed. About 50 percent of those reports reflected transactions of $20,000 or less. This produces a vast amount of financial intelligence.

SARs highlight suspicious behavior and point us to indicators of potential criminal activity—such as structuring and other forms of money laundering. They may be the only hook we have to detect a terrorist cell.

CTRs help fill out the financial intelligence picture because of the objective criteria for filing them. Rather than a subjective analysis of financial behavior, they document specific transactions and patterns of activity that may be the crucial piece of evidence to a case.

CTRs actually provide financial intelligence on more subjects than SARs reporting alone. One tool is not a substitute for the other. SARs and CTRs work in concert together—and together, they are a powerful weapon. Obviously, they provide information about specific transactions. But they provide a much bigger picture than just isolated transactions. They fill in biographical or geographical information—which might let us prove where a suspect was on a particular day. They help us develop leads to expand our investigations. They can link people and accounts conclusively together—connections we might not otherwise see.

Let me give you an example. Some of you may have heard of the Al Haramain Islamic Foundation. It was a charity based in Saudi Arabia, with branches all over the world. Its U.S. branch was established in Oregon in 1997 and in 1999, it registered as a 501(c)(3) charity.

In 2000, the FBI discovered possible connections between Al Haramain and al Qaeda and began an investigation. We started where we often start—by following the money. And we uncovered criminal tax and money laundering violations.

Al Haramain claimed that money was intended to purchase a house of prayer in Missouri—but in reality, the money was sent to Chechnya to support al Qaeda fighters.

In 2004, the Treasury Department announced the designation of the U.S. branch of Al Haramain, as well as two of its leaders, and several other branch offices. In 2005, a federal grand jury indicted Al Haramain and two of its officers on charges of conspiring to defraud the U.S. government.

We relied on BSA information and cooperation with financial institutions for both the predication and fulfillment of the investigation. Because of reporting requirements carried out by banks, we were able to pursue leads and find rock-solid evidence.

Yes, we used other investigative tools—like records checks, surveillance, and interviews of various subjects. But it was the financial evidence that provided justification for the initial designation and then the criminal charges.

That's why your cooperation is so vital—and that of the Treasury Department as well. As in the case I just discussed, together we have frozen the assets of at least 440 suspected and known terrorists or terrorist organizations. We couldn't have done this without the diligence and dedication of the financial institutions that carry out these designations. It is difficult to measure success in convictions of terrorist financiers because of the variety of violations we may use to charge suspects. But it is safe to say that any convictions we achieve absolutely depend on banking information.

So when your bank's officers are conducting reportable transactions, there are some things they can do to help us glean even more information right off the bat. Let me just run through a few:

. You can complete each applicable field.

. You can verify personal identifiers, where possible, and even complete the "description" narrative. When you fill out the "who, what, when, where, why, and how" on the front end, this saves us all time on the back end, because we don't have to come back to you with subpoenas, looking for specific information.

. You can check all the violation types that apply and avoid checking the "other" box.

. Finally, you can file the reports electronically, which will save all of us time.

. And if a customer strikes you as especially suspicious, call us in addition to filing a SAR.

Believe me, we know that this creates a lot of work for you. We also know you don't necessarily see an obvious return on your investment. But these reports do help us. They often become the cornerstones of our cases. Concrete connections are made by things as innocuous as learning the name of an account's co-signer. The more information we have, the more we have to go on. When we can follow the money, we stand a much better chance of breaking a case wide open.

All of this requires tremendous effort from us all—from your employees and from the FBI's employees. But this cooperation does more than just help us find terrorists and bring them to justice. It helps us all protect the integrity of financial institutions.

* * *

Before I conclude, I want to take a moment to talk about another area of risk, and another way that collaboration can help reduce that risk—and that is in the cyber arena.

We know that terrorists want to wreak havoc on our society, whether by outright attacks on our lives or attacks on our economy. One way in is through cyberspace. Your companies face external risks from terrorists hacking your systems and internal risks from trusted insiders.

We know that hackers have exfiltrated huge amounts of data from the systems of various companies and institutions. The U.S. government is taking strong steps to help shore up vulnerabilities in the .com, .gov, and .edu worlds, and we have identified a number of perpetrators and hardened a number of targets. But as you know, there are always those who are searching for still more vulnerabilities.

Yes, it is your responsibility to protect your systems, but we can help you. Our InfraGard program is a partnership between the FBI and private companies that works to help all of us protect our infrastructure. About two-thirds of Fortune 500 companies are represented, and if you're not a member, we urge you to become one. The InfraGard program lets us share information in a trusted environment on everything from computer intrusions to extortion. If we are all on the same page, we can work with you to investigate the source of the attack and help you guard against another one.

You also face threats from trusted insiders. What if al Qaeda or another foreign sponsor were able to infiltrate someone into your company, perhaps as an IT specialist or systems administrator? The FBI has certainly had a number of applicants for these jobs. Their goal is to get through our screening and get access to our systems. This would be just as dangerous as a truck bomb exploding. These insiders are sophisticated and must be closely watched. Otherwise, they could take down your system, compromise other companies, and cause grave and widespread economic damage.

We all want to protect the privacy of our clients and citizens, yet we also want to protect their security and their lives.

* * *

And so we need to continue our cooperation—and strengthen it. Because more challenges loom ahead, for all of us.

Globalization and technology present new complications. Stored value cards lack regulation and permit both anonymity and easy transportation of funds. Internet banking also opens up new channels for those wishing to make anonymous transactions. And online payment services don't have even basic customer identification and record-keeping regulations.

And on the opposite end of the technology spectrum, we expect to see cash couriers who can move money without the oversight your institutions provide.

Our adversaries will either become more technologically savvy or they will regress to methods that don't leave a paper trail. We can't predict what they will do. But we can do everything in our power to make it more difficult for them.

Tightening our financial systems works to our advantage and to our enemies' disadvantage. The more we work together, the more we deny them the ability to work in secret and force them to be creative. And the more they are forced to take risks and find ways around our systems, the higher the likelihood they will slip up.

And if they do, we will be waiting to catch them. The threat is real, and the stakes are high. We must not fail. And working together, we will not fail.

# # #

EXHIBIT T

PUBLIC UNCLASSIFIED BRIEF

No. 06-36083
(Consolidated with Nos. 06-17132, 06-17137)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AL-HARAMAIN ISLAMIC FOUNDATION, INC., et al.,
Plaintiffs - Appellees,

v.

GEORGE W. BUSH, et al.,
Defendants - Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF FOR APPELLANTS

PAUL D. CLEMENT
Solicitor General

GREGORY G. GARRE
Deputy Solicitor General

DARYL JOSEFFER
Assistant to the Solicitor General

PETER D. KEISLER
Assistant Attorney General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

STATEMENT OF THE ISSUE

Plaintiffs, a terrorist organization and two lawyers affiliated with it, contend that they were subjected to warrantless electronic surveillance under the now-discontinued Terrorist Surveillance Program ("TSP"). The district court recognized that the Government had properly invoked the state secrets privilege, and that it remains secret whether plaintiffs were actually subject to any surveillance. The question presented is whether the district court erred in nonetheless declining to dismiss the case, and instead calling for *in camera* proceedings that could risk the disclosure of state secrets.

STATEMENT OF THE CASE

Plaintiffs are Al-Haramain Islamic Foundation, Inc., an entity designated by the United States and the United Nations as a terrorist organization, and two lawyers affiliated with Al-Haramain. Plaintiffs alleged that they were subjected to warrantless foreign intelligence surveillance under the TSP, which the President authorized in the aftermath of the September 11, 2001 attacks to protect against future terrorist attacks. ER 501-08. The Government formally invoked the state secrets privilege and moved for dismissal or summary judgment because the very subject matter of this action is a state secret and the case cannot be litigated without recourse to highly classified state secrets concerning foreign intelligence gathering.

In response, the Government asserted the state secrets privilege and related statutory privileges, and moved for dismissal or summary judgment. See Motion to Dismiss Or, In the Alternative, For Summary Judgment (June 21, 2006). The state secrets privilege, which must be invoked by the pertinent agency head, requires dismissal whenever "there is a reasonable danger" that disclosing information in court proceedings would harm national security interests, such as by disclosing intelligence-gathering methods or capabilities. See *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). Dismissal is required if the action's "very subject matter" is a state secret, or if the plaintiff cannot prove a *prima facie* case, or the defendant cannot establish a valid defense, without information protected by the privilege. See *ibid.*

The Government's motion was supported by public and classified declarations of the then-Director of National Intelligence, John Negroponte, and the NSA's Director, General Keith Alexander. The Government also filed public and *ex parte/in camera* briefs, explaining that it could neither confirm nor deny whether plaintiffs had been surveilled under the TSP or any other intelligence-gathering program, and that litigation of plaintiffs' claims threatened disclosure of intelligence information, sources, and methods. See Mem. In Support of Motion (June 21, 2006).

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 7]

098

EXHIBIT U

Exh. 156
#2

KARIN J. IMMERGUT, OSB #963143
United States Attorney
District of Oregon
CHRISTOPHER L. CARDANI
Assistant United States Attorney
701 High Street
Eugene, OR 97401
(541) 465-6771
chris.cardani@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA, Plaintiff, v. PEROUZ SEDAGHATY, a/k/a Pete Seda and Abu Yunus, Defendant.	No. CR 05-60008-01 GOVERNMENT'S MEMORANDUM IN SUPPORT OF PRETRIAL DETENTION

The United States of America, through its undersigned counsel, herein submits this memorandum in advance of defendant Sedaghaty's detention hearing, scheduled for Wednesday, August 22, 2007.

Despite defendant's voluntary return to the United States, the government believes that no set of conditions can be imposed upon defendant Sedaghaty that will reasonably assure the safety of the community and his appearance at trial. Support for this position is drawn from this memorandum, exhibits submitted with this memorandum, and from testimony anticipated at the detention hearing.

Your brothers, the Mujahideens (Ussamah Bin Laden Brigade).

Visit our site at www.laden.s5.com/ladenindex.htm

Although it is unknown who authored this message, it was dated October 10, 2001, which is three days after the United States began bombing Afghanistan after the terrorist attacks of 9-11. Testimony at the detention hearing will provide more context to this troubling e-mail.

The images and writings reviewed above, when considered in conjunction with the actions of defendant Sedaghaty, show that he not only ideologically agrees with the efforts of the *mujahideen,* but has supported them with funding and other types of logistical support from within the United States. Witting facilitation of radical Islamist fighters, and the distribution of hateful, violent literature to prisoners exhorting violence, makes defendant Sedaghaty a danger to the community.

Flight Risk

Defendant Sedaghaty departed the United States shortly after he was interviewed by the FBI in February 2003 and, so far as the government is aware, he did not return to the United States until four and a half years later, on August 15, 2007. While away from the United States, he retained a criminal defense attorney in Oregon to represent him during the criminal investigation. This attorney met with criminal investigators and the prosecutor both prior to and after defendant Sedaghaty was indicted.

Events significant to the timeline of defendant's absence from this country include:

February 2003 - Sedaghaty interviewed by the FBI and departs shortly

		thereafter
February 2004	-	Law enforcement execute search warrant at AHIF-US building in Ashland, Oregon
February 2004	-	OFAC issued a preliminary designation of AHIF-US as an SDGT (public notice provided)
June 2004	-	The Kingdom of Saudi Arabia dissolved AHIF-SA.
September 2004	-	OFAC and the UN issue a formal designation of AHIF-US and defendant Al-Buthe as terrorist supporters
February 2005	-	AHIF-US and defendants Sedaghaty and Al-Buthe indicted by a federal grand jury in Eugene, Oregon. This Court issues arrest warrants.
August 15, 2007	-	Defendant Sedaghaty is arrested at the Portland, Oregon International Airport after voluntarily returning to the United States.

Defendant Sedaghaty's criminal defense attorney met with defendant Sedaghaty outside the United States while he was a fugitive.[8] Defendant Sedaghaty has known that he was indicted and the subject of an arrest warrant for at least two and a half years.[9]

---

[8]To be clear, Sedaghaty was not a fugitive when he left the United States in 2003; he became a fugitive by operation of law when he was indicted in 2005, and the arrest warrant was issued, which defendant Sedaghaty had knowledge of while abroad.

[9]Exhibit P is an Associated Press article appearing on February 20, 2005, and states in part: "Lynne Bernabei, the Washington, D.C. lawyer representing Seda, Al-Buthe and Al-Haramain's Ashland chapter in the terrorist designation case, told the (Medford) Mail-Tribune that Seda is familiar with the charges against him and will return

EXHIBIT V

Congress v. Your Privacy
Warrantless spying bill passes
Support the ACLU lawsuit
www.aclu.org/fisaaction

Surveillance Documentary
Freedom Files Sneak Preview
Watch a video on wiretapping issues
www.ACLU.tv

Search FBI Records
Instant FBI records lookup. FBI records online database.
FBI.GovtRegistry.com

Patriot Act Assessmen
Providing Banks with exp
BSA,AML OFAC & Patriot
Assessments
www.BSAstrategies.com

V V

Ads t

Statement
United States Senate Committee on the Judiciary
FISA for the 21st Century
July 26, 2006

General Michael V. Hayden
Director of Central Intelligence , Central Intelligence Agency

Testimony to the Judiciary Committee of the US Senate
By General Michael V. Hayden,
Director, CIA

26 July 2006

Mister Chairman, Senator Leahy, thank you for the opportunity to speak before your committee today. The work that you and we have before us is truly important: how dowe best balance our security and our liberty in the pursuit of legitimate foreign intelligence. Let me congratulate the Committee for taking on the task of examining and--where appropriate--amending the Foreign Intelligence Surveillance Act.

This task of balancing liberty and security is one that those of us in the intelligence community take very seriously and one to which we constantly turn our attention.

I recall that within days of the 9-11 attacks I addressed the NSA workforce to lay out our mission in a new environment. It was a short video talk beamed throughout our headquarters at Fort Meade and globally. Most of what I said was what anyone would expect. I tried to inspire. Our work was important and the Nation was relying on us. I tried to comfort. Look on the bright side: right now a quarter billion Americans wished they had your job. I ended the talk by trying to give perspective. All free peoples have had to balance the demands of liberty with the demands of security. Historically we Americans had planted our flag well down the spectrum toward liberty. Here was our challenge. "We were going to keep America free," I said, "by making Americans feel safe again."

This was not an easy challenge. The Joint Inquiry Commission (comprised of the House and Senate Intelligence Committees) would summarize our shortcomings in the months and years leading to the September 11th attacks. The Commission harshly criticized our ability to link things happening in the United States with things that were happening elsewhere.

Let me note some of JIC's Systemic Findings (Joint HPSCI-SSCI, from abridged findings and conclusions)

"...NSA's cautious approach to any collection of intelligence relating to activities in the United

States" (finding 7)

"There were also gaps in NSA's coverage of foreign communications and the FBI's coverage of domestic communications" (Finding 1, p 36, tab 4)

"...NSA did not want to be perceived as targeting individuals in the United States." (Finding 1, p 36, tab 4)

"[in talking about one end US conversations]...there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland." (Finding 1, p. 36, tab 4)

For NSA the challenge was especially acute. NSA intercepts communications and it does so for only one purpose: to protect the lives, the liberties and the well being of the citizens of the United States from those who would do us harm. By the late 1990s, that job was becoming very difficult. The explosion of modern communications in terms of its volume, variety and velocity threatened to overwhelm the Agency.

The September 11th attacks exposed an even more critical fault line. The laws of the United States do (and should) distinguish between the information space that is America and the rest of the planet.

But modern telecommunications do not so cleanly respect that geographic distinction. We exist on a unitary, integrated, global telecommunications grid in which geography is an increasingly irrelevant factor. What does "place" mean when one is traversing the World Wide Web? There are no area codes on the Internet.

And if modern telecommunications muted the distinctions of geography, our enemy seemed to want to end the distinction altogether. After all, he killed 3000 of our countrymen from within the homeland.

In terms of both technology and the character of our enemy, "in" America and "of" America no longer were synonymous.

I testified about this challenge in open session to the House Intelligence Committee in April of the year 2000. At the time I created some looks of disbelief when I said that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, there were provisions of US law that would kick in, offer him some protections and affect how NSA could now cover him. At the time I was just using this as a stark hypothetical. Seventeen months later this was about life and death.

The legal regime under which NSA was operating--the Foreign Intelligence Surveillance Act--had been crafted to protect American liberty and American security.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute was optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

Because of the wording of the statute, the government looks to four factors in assessing whether or not a court order was required before NSA can lawfully intercept a communication: who was the target, where was the target, how did we intercept the communication, and where did we intercept the communication.

The bill before the committee today effectively re-examines the relevance of each of these factors and the criteria we want to use with each.

Who is the target?

The FISA regime from 1978 onward focused on specific court orders, against individual targets, individually justified and individually documented. This was well suited to stable, foreign entities on which we wanted to focus for extended period of time for foreign intelligence purposes. It is less well suited to provide the agility to detect and prevent attacks against the homeland.

In short, its careful, individualized processes exacted little cost when the goal was long term and exhaustive intelligence coverage against a known and recognizable agent of a foreign power. The costs were different when the objective was to detect and prevent attacks, when we are in hot pursuit of communications entering or leaving the United States involving someone associated with al Qa'ida.

In this regard, extending the period for emergency FISA's to seven days and allowing the Attorney General to delegate his authority to grant emergency orders is also very welcome and appropriate.

Where is the target?

As I said earlier, geography is becoming less relevant. In the age of the Internet and a global communications grid that routes communications by the cheapest available bandwidth available each nanosecond, should our statutes presume that all communications that touch America should be equally protected?

As the Chairman noted earlier this week, we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that gets routed through US facilities.

Our limited government resources should focus on protecting US persons, not those entities who get covered as a result of technological changes that extend the impact--and protection--of FISA far beyond what its drafters intended.

I know that Senator DeWine among others has been very concerned about allocations of these resources and FISA backlogs. As Director of CIA I share his concerns in allocating my resources and hope that this legislation will help properly focus resources on protecting the legitimate privacy rights of US persons.

How did we intercept the communication?

For reasons that seemed sound at the time, current statute makes a distinction between collection "on a wire" and collection out of the air. When the law was passed, almost all local calls were on a wire and almost all long haul communications were in the air. In an age of cell phones and fiber optic cables, that has been reversed...with powerful and unintended consequences for how NSA can lawful acquire a signal. Legislators in1978 should not have been expected to predict the future of global telecommunications. Neither should you. The statute should be technology neutral.

Where we intercept the communication?

106

A single communication can transit the world even if the communicants are only a few miles apart. And in that transit NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication--one that would help protect the homeland, for example--is always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.

In that light, there are no communications more important to the safety of the Homeland than those affiliated with al Qa'ida with one end in the United States. And so why should our laws make it more difficult to target the al Qa'ida communications that are most important to us--those entering or leaving the United States!

Because of the nature of global communications, we are playing with a tremendous home field advantage and we need to exploit this edge. We also need to protect this edge and those who provide it. The legislative language requiring compulsory compliance from carriers is an important step in this regard.

After 9/11, patriotic Americans assisted the Intelligence Community in ensuring that we have not had another attack on our soil since that awful day. And prior to 9/11, we received critical assistance across the IC from private entities. As Director of NSA, Deputy DNI, and now Director of the CIA, I understand that government cannot do everything. At times, we need assistance from outside the government.

Whatever legal differences and debates may occur about separation of powers, Article 2, and so on, those people who provide help to protect America should not suffer as a part of this debate. I would urge the committee to recognize the importance of the efforts of these Americans and provide appropriate protection.

One final--and very important--point. Many of the steps contained in the proposed legislation will address the issue raised by the Congress' Joint Inquiry Commission: one end US conversations, communications that the JIC characterized as "among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland."

That means NSA will bump up against information to, from or about US persons. Let me stress that NSA routinely deals with this challenge and knows how to do this while protecting US privacy. The draft bill contains quite a bit of language about minimization--the process NSA uses to protect US identities. The same rules of minimization that NSA uses globally, rules approved by the Attorney General and thoroughly briefed to Congress, will be used.

Let me close by saying that we have a great opportunity here today. We can meet the original intent of the FISA Act to protect our liberty and our security by making the legislation relevant to both the technologies and the enemies we face.

Thank you.